

CLAIMS

1. Process for ensuring the secure transmission of a message from a transmitter (1) to a receiver (2), in which the transmitter generates and integrates into the message a signature so as to produce a signed message, characterized by the fact that said process consists of the following stages:

- the transmitter associates with the signed message transmission checking information (IDEM) deriving from the signed message according to a specified law, and

- the transmitter generates and transmits (105) to the receiver data that represent the signed message and the transmission checking information (IDEM), and the receiver:

- receives said transmitted data,

- determines (204), according to said law, reception checking information (IDEM') deriving from the message received, and

- compares (205) reception checking information (IDEM') against the transmission checking information (IDEM) in order to validate the message received in the event that they coincide.

2. Process according to Claim 1, wherein said law implements a mathematical function.

3. Process according to one of Claims 1 and 2, wherein the transmitter additionally generates and transmits transmitter identification information (CRYPT_IDENT or IDENT_SPY) that was used to personalize said law, and the receiver likewise personalizes the law according to the transmitter identification information

(CRYPT_IDENT or IDENT_SPY) that is received in order to determine the reception checking information.

4. Process according to one of Claims 1-3, wherein the transmitter sets up said law such that the transmission checking information (IDEM) is representative of at least one kind of information that is selected from within the group composed of message consistency information (X') and message meaning information (Y').

5. Process according to Claims 3 and 4 together, wherein the message consistency information (X) is determined by a first quotient that is provided by dividing the transmitter identification information (IDENT_SPY) by a number of characters contained in the message.

6. Process according to Claim 5, wherein a first remainder that is obtained by the above-mentioned division step is itself divided by a first number in order to obtain a second quotient and a second remainder, whereby the second remainder is added to a constant to obtain a predetermined number of characters, message consistency characters, after conversion into a base that is selected from among a set of conversion bases.

7. Process according to Claim 6, wherein the remainder from the second quotient is divided by a first number in order to obtain a third quotient that is associated with a third remainder whose value is added to a constant value to obtain the message consistency information (X').

8. Process according to Claim 7, wherein the first number is 46027 and the constant is 4623.

9. Process according to one of Claims 4 to 8, wherein the message consistency information (X') is represented by characters, the number of which is below a threshold that represents a specified percentage relative to a size of the transmitted data.

10. Process according to one of Claims 3 and 4 together, wherein the message meaning information (Y') is determined by adding up a specified number of alphanumeric characters of the message, whereby each alphanumeric character has a value that is twice the ASCII value that is representative of the character in question, minus an ASCII value that is representative of an adjacent character, whereby the resulting sum is taken as a divisor of a dividend, which is the transmitter identification information (IDENT_SPY), so as to provide the message meaning information.

11. Process according to one of Claims 4 to 10, wherein the message meaning information (Y') is represented by characters, the number of which is below a threshold that represents a specified percentage relative to a size of the transmitted data.

12. Process according to one of Claims 3 to 11, wherein the transmitter identification information (IDENT_SPY) is obtained:

by a stage for transcoding of strings, of specified sizes, of alphanumeric characters that represent data fields to be protected, thus providing a first set of intermediate results, each of which has a specified number of digits, and

a stage for transforming the first set of intermediate results by means of a transformation algorithm (As) that is randomly selected from among a set of algorithms (s), each of which uses an alphanumeric-character base that is particular to the algorithm in question in order to obtain a final result (IDENT_SPY) after a conversion matrix is

used to convert the characters of the alphanumeric base of the selected algorithm into characters having numerical values of a predetermined base.

13. Process according to Claim 12, wherein the transmitter identification information (IDENT_SPY) is transmitted in encoded form by transforming the transmitter identification information, in a specified base, into an encoded result that has a specified number of digits expressed in a mathematical base (Y) that is randomly selected from a set (V) of conversion bases in order to obtain an encoded identifier of the transmitter (CRYPT_IDENT) wherein information (Y), identifying the selected mathematical base, is inserted at a variable rank (r) that is specified by a pointer (Z) that is inserted at a rank (W) for which the receiver has information for determining said rank.

14. Process according to Claim 13, wherein the rank (r) of the information (Y) for identifying the selected mathematical base is defined by an integer quotient that is obtained by dividing a particular value, which is associated with the pointer (Z) by a table, by a number (s) that specifies the size of the set of algorithms (As).

15. Process according to one of Claims 13 and 14, wherein the rank (W) of the pointer (Z) is inserted at a rank that is calculated by taking the sum, modulo 9, of ASCII codes of said intermediate result that represents terms that specify a mathematical function that determines the transmitter identification information (IDENT_SPY).

16. Process according to one of Claims 14 and 15, wherein the receiver:

- calculates the sum of the ASCII codes of at least one block of data of the above-mentioned alphanumeric data field, whereby said block is received in the transmitter identification information,

- expresses said sum in modulo 9, to determine the rank (W) of the pointer (Z),

- reads said pointer (Z) that is received, and

- calculates the rank (r) of the identification information (Y) of the selected mathematical base by dividing the particular value associated with the pointer (Z) by the value (s) that represents the size of the set of algorithms as expressed in a predetermined base, and

- exploits the encoded information received (CRYPT_IDENT) after eliminating therefrom the identification information (Y) of the selected mathematical base and the pointer (Z).

17. Process according to one of Claims 1 to 16, wherein said data are transmitted to the receiver via a data storage system.

18. Process according to Claim 17, wherein the receiver (2) is also the transmitter (1).

19. System for securing the implementation of the process of one of Claims 1 to 18, comprising a transmitter (1) that is associated with a receiver (2), whereby the transmitter is designed to generate and integrate with the message a signature so as to produce a signed message, wherein:

the transmitter (1) contains:

- means (103, 104) for generating and associating with the signed message transmission checking information (IDEM) deriving from the signed message according to a specified law, and

- means (105) for sending to the receiver (2) data that represent the signed message and the transmission checking information (IDEM),

and the receiver (2) contains:

- means for receiving said transmitted data,
- means (203, 204) for determining, according to said law, reception checking information deriving from the message received, and
- means (205) for comparing the reception checking information against the transmission checking information (IDEM) in order to validate the received message in the event that they coincide.

20. Security system according to Claim 19, wherein the transmission means (105) are also controlled by means (103) for generating the transmitter identification information (CRYPT_IDENT or IDENT_SPY) that was used to personalize said law, and the receiver likewise contains means for personalizing the law, according to the transmitter identification information (CRYPT_IDENT or IDENT_SPY) that was received by the reception means, which control the means (204) for determining the reception checking information.

21. Security system according to one of Claims 19 and 20, wherein the transmitter is designed (104) such that said law ensures that the transmission checking information (IDEM) is representative of at least one kind of information that is selected from among the group that consists of the message consistency information and the message meaning information.

22. Data medium that contains a set of software for controlling a computer system for the purpose of implementing the process of one of Claims 1 to 18, whereby the set of software contains at least one of the following two subsets:

a first subset for the transmitter that contains software for controlling the system for associating with the signed message the transmission checking information (IDEM)

deriving from the signed message according to a specified law, and software for controlling the generation and transmission (105) to the receiver of the data that represent the signed message and the transmission checking information (IDEM), and

a second subset for the receiver that contains software for receiving the above-mentioned transmitted data, software (204) for determining, according to said law, the reception checking information (IDEM') deriving from the received message, and software (205) for comparing the reception checking information (IDEM') against the transmission checking information (IDEM) in order to validate the received message in the event that they coincide.

23. Software medium according to Claim 22, wherein the first subset additionally contains software for generating and transmitting the transmitter identification information (CRYPT_IDENT or IDENT_SPY) that was used to personalize said law, and the second subset likewise contains software for personalization according to this same law based on the transmitter identification information (CRYPT_IDENT or IDENT_SPY) that is received in order to determine the reception checking information.

24. Data medium according to one of Claims 22 and 23, wherein said law is set up such that the transmission checking information (IDEM) is representative of at least one kind of information that is selected from the group that consists of the message consistency information (X') and the message meaning information (Y').

25. Data medium according to one of Claims 22 to 24, consisting of a chip card.